(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－44642

(43)公開日　平成８年(1996)２月16日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　13/00	３５１　Ｍ	7368－5E		
	３５３　Ｔ	7368－5E		
	３５５	7368－5E		
Ｈ０４Ｌ　12/56				
		9466－5K	Ｈ０４Ｌ　11/ 20　１０２　Ａ	

審査請求　未請求　請求項の数21　ＦＤ　（全 18 頁）

(21)出願番号　特願平6－333261

(22)出願日　平成６年(1994)12月15日

(31)優先権主張番号　１６８０４１

(32)優先日　1993年12月15日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　595008191
チェックポイント、ソフトウェアー、テクノロジーズ、リミテッド
CHECKPOINT SOFTWARE TECHNOLOGIES, LTD.
イスラエル国ラマト－ガン、アバ、ヒレル、シルバー、ロード、７、シルバー、ハウス

(72)発明者　ギル、シウェド
イスラエル国エルサレム、ピライク、ストリート、６

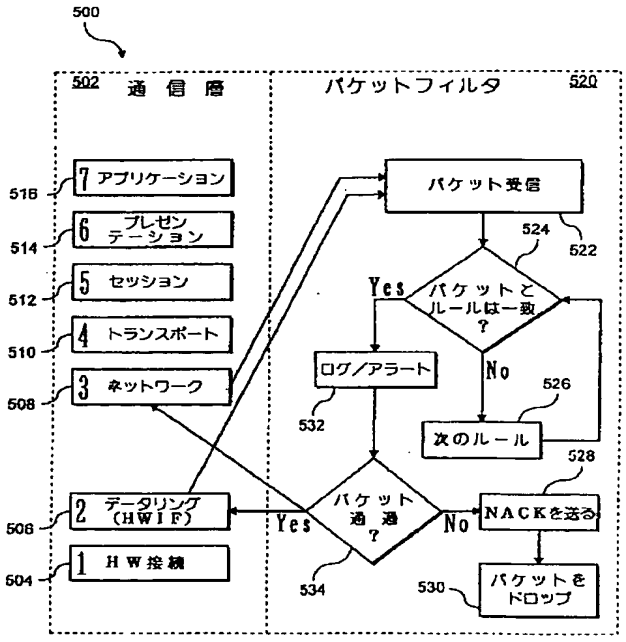
(74)代理人　弁理士　佐藤　一雄　（外３名）

(54)【発明の名称】　コンピュータネットワークの制御方法及び保安システム

(57)【要約】

【目的】　コンピュータネットワーク上の情報の流れを制御する、フレキシブルで容易に変更可能な保安方法の提供。

【構成】　フィルタモジュールがネットワーク内のトラヒックについての保安ルールを特定しそしてこの保安ルールに従って通信パケットを受け入れまたは落とすことによりネットワークの安全性を制御する。一群の保安ルールがハイレベル形式で定義されそしてパケットフィルタコードに変換される。このパケットフィルタコードはネットワーク内の戦略的な点に置かれたパケットフィルタモジュールにロードされる。これら位置に送られまたは入る各パケットはパケットフィルタコード内の命令を実行することで検査される。パケットフィルタコード演算の結果がパケットを受け入れる（パス）か排除（ドロップ）して通信の試みを不能とするかを決定する。



1

【特許請求の範囲】

【請求項１】データがデータパケットとして扱われるコンピュータネットワークにおける上記データパケットの伝送を保安ルールに従って制御するための、下記段階を含む方法：

ａ）保安ルールにより制御される上記ネットワークの夫々のアスペクトの定義を発生する段階；

ｂ）上記アスペクトの内の少くとも一つを制御するために上記アスペクト定義で上記保安ルールを発生する段階；

ｃ）上記データパケットの伝送を制御するパケットフィルタリングモジュールの動作を制御するために上記保安ルールを一セットのフィルタ言語命令に変換する段階；

ｄ）上記ルールに従って上記データパケットの伝送を制御するために、パケットフィルタリング仮想計算機をつくるパケットフィルタモジュールを少くとも一つのネットワークエンティティに設ける段階；

ｅ）上記ネットワーク内の上記パケットの伝送を許可または拒否するために上記パケットフィルタリングモジュール仮想計算機を動作させるために上記モジュールが上記命令を読取りそして実行する段階。

【請求項２】前記アスペクトはネットワークオブジェクトを含む請求項１の方法。

【請求項３】前記アスペクトはネットワークサービスを含む請求項１の方法。

【請求項４】前記アスペクトはネットワークサービスを含む請求項２の方法。

【請求項５】前記オブジェクト定義は前記オブジェクトのアドレスを含む請求項４の方法。

【請求項６】前記段階ｃ）のフィルタ言語命令はスクリプトの形であり、更にこのスクリプトを前記段階ｅ）で実行される前記命令にコンパイルするためのコンパイラを含む請求項１の方法。

【請求項７】前記段階ａ）およびｂ）において、前記ネットワークのアスペクトおよび前記保安ルールのアスペクトが図形的に定義されるごとくなった請求項１の方法。

【請求項８】データがデータパケットとして伝送されるコンピュータネットワーク用の保安システムであって、保安ルールに従って上記ネットワーク内の上記データパケットの伝送を制御し、この保安ルールにより制御される上記ネットワークの各アスペクトをこの保安ルールがそれらアスペクトで定義しそしてフィルタ言語命令に変換するようになった保安システムにおいて、下記段階を含む上記システムを動作させる方法：

ａ）上記保安ルールにより制御されるべき上記ネットワークの少くとも１つのエンティティに、上記データパケットの伝送を制御するパケットフィルタリング仮想計算機をつくるパケットフィルタモジュールを設ける段階；

ｂ）上記ネットワーク内の上記パケットの伝送を許可または拒否するために上記パケットフィルタリングモジュールを動作させるために、上記モジュールが上記命令を読取りそして実行する段階。

2

【請求項９】前記アスペクトはネットワークオブジェクトを含む請求項８の方法。

【請求項１０】前記アスペクトはネットワークサービスを含む請求項８の方法。

【請求項１１】前記アスペクトはネットワークサービスを含む請求項９の方法。

【請求項１２】前記オブジェクト定義は前記オブジェクトのアドレスを含む請求項１１の方法。

【請求項１３】前記仮想計算機はデータ抽出動作を行うごとくなった請求項８の方法。

【請求項１４】前記仮想計算機は論理動作を行うごとくなった請求項１３の方法。

【請求項１５】前記仮想計算機は比較動作を行うごとくなった請求項１４の方法。

【請求項１６】データがデータパケットとして伝送されるコンピュータネットワーク用の保安システムであって、保安ルールに従って上記ネットワーク内の上記データパケットの伝送を制御し、この保安ルールにより制御される上記ネットワークの各アスペクトをこの保安ルールがそれらアスペクトで定義しそしてフィルタ言語命令に変換するようになった保安システムであって、下記段階を含む上記システムを動作させる方法：

ａ）上記保安ルールにより制御されるべき上記ネットワークの少くとも１つのエンティティに、上記データパケットの伝送を制御するパケットフィルタリングモジュールをエミュレートするパケットフィルタモジュールを設ける段階；

ｂ）パケットフィルタリング動作用に上記モジュールが命令を読取りそして実行する段階；

ｃ）上記段階ｂ）の結果を記憶装置に記憶する段階；

ｄ）上記ネットワーク内の上記パケットの伝送を許可しまたは拒否するために上記パケットフィルタモジュールを動作させるために、上記命令を上記モジュールが読取って実行しそして上記記憶された結果を利用する段階。

【請求項１７】前記アスペクトはネットワークオブジェクトを含む請求項１６の方法。

【請求項１８】前記アスペクトはネットワークサービスを含む請求項１６の方法。

【請求項１９】前記アスペクトはネットワークサービスを含む請求項１７の方法。

【請求項２０】前記オブジェクト定義は前記オブジェクトのアドレスを含む請求項１９の方法。

【請求項２１】データがデータパケットとして伝送されるコンピュータネットワーク用の保安システムであって、保安ルールに従って上記ネットワーク内の上記データパケットの伝送を制御し、この保安ルールにより制御される上記ネットワークの各アスペクトを定義しそして

フィルタ言語命令に変換するようになった保安システムにおいて、下記要件を含む保安装置：

ａ）上記保安ルールにより制御されるべき上記ネットワークの少くとも１個のエンティティに、上記データパケットの伝送を制御するパケットフィルタリング仮想計算機をつくるパケットフィルタモジュールを設ける手段；

ｂ）上記モジュール内にあって、上記ネットワーク内の上記パケットの伝送を許可しまたは拒否するために上記パケットフィルタリングモジュールを動作させるために、上記命令を読取りそして実行するための手段。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は一般にコンピュータネットワークの安全性を制御する方法に関し、詳細には外部および内部の宛先に対するネットワーク上の情報の流れを制御するコンピュータネットワークの保安のための容易に変更可能なまたは拡張可能な方法に関する。

【０００２】

【従来の技術】殆どの組織の計算環境において、接続性と保安性は二つの矛盾する対象物である。典型的な現代の計算システムは多数のサービスに対して即応型のアクセスを与えるネットワーク通信に関してつくられる。これらサービスの大域的な使用の可能性はおそらく現代の計算の解の唯一最重要な特徴である。接続性の要求は組織内からそしてその外側からも入る。

【０００３】

【発明が解決しようとする課題】許可のない使用についてネットワークサービスを保護することはいずれの組織にとっても重要なことである。例えばＵＮＩＸワークステーションは一旦インターネットに接続されると全世界に、次のテーブル上の他のステーションにそれが提供するサービスのすべてを提供することになる。現在の技術を用いれば、一つの組織は、外部世界または他のサイトへのすべての接続を解消する程度にさえ弱点の防止のためにその接続性の殆どを放棄しなければならない。

【０００４】保安要求の増大に伴い、ネットワーク資源へのアクセスを制御するための手段が管理上で優先的なものとなっている。コストを節約し製造性を維持するために、アクセス制御はその構成が単純であり、ユーザおよびアプリケーションに対し透明でなくてはならない。機械設備のコストの低減とダウン時間の短縮も重要な因子である。

【０００５】パケットフィルタリングはトラヒックを制御することにより、保安性を与えつつ接続性を可能にして、単一ネットワーク内および接続ネットワーク間の不法な通信の試みを防止する一つの方法である。

【０００６】パケットフィルタリングの現在の実行は固定フォーマットに従ってのアクセスリストテーブルの仕様を可能にする。この方法は与えられた組織の保安ポリシーを表わすについてのそのフレキシビリティに限界がある。またこれは特定のテーブル内に限定されたプロトコルおよびサービス群に制限される。この方法は元のテーブルに特定されていない、異なるプロトコルまたはサービスの導入を許さない。

【０００７】パケットフィルタリングを実行するための他の方法は組織内の戦略的なポイント毎にコンピュータオペレーティングシステムコートを手動的に調整するものである。この方法はネットワークトポロジーの将来の変更、新しいプロトコル、向上したサービス、およびそこでの将来の保安性に対するそのフレキシビリティに限界がある。これは所有するコンピュータプログラムの変更にエキスパートによる多量のワークを必要とし、その構成と維持を不充分且つ安価なものにする。

【０００８】本発明の目的はコンピュータネットワーク上の情報の流れを制御する、フレキシブルで容易に変更可能な保安方法を提供することである。

【０００９】本発明の他の目的は内部並びに外部の宛先についてネットワーク上の情報の流れを制御する方法を提供することである。

【００１０】本発明の更に他の目的はパケットを許可（パス）または拒否（ドロップ）するために一つのノードの与えられた保安ポリシーを実行するために一組の命令により制御される一般的なパケットフィルタモジュールを提供することである。

【００１１】更に他の目的はパケットフィルタ自体の性質を変える必要なくあるいは長いコードを書込む必要なしにシステム管理プログラムにより容易に変更しうる、コンピュータネットワーク用の保安方法を提供することである。

【００１２】

【課題を解決するための手段】これらおよび他の目的、特徴および利点は、データがデータパケットとして伝送されるコンピュータネットワークを動作させるための、保安ルールに従ってそのネットワーク内のデータパケットの流れを制御するための方法であって、保安ルールにより制御されるネットワークの夫々のアスペクトの定義を発生する段階、上記アスペクトの内の少くとも一つを制御するために上記アスペクト定義で上記保安ルールを発生する段階、上記データパケットの流れを制御するパケットフィルタリングモジュールの動作を制御するために上記保安ルールを一セットのフィルタ言語命令に変換する段階、上記ルールに従って上記データパケットの流れを制御するために、パケットフィルタリング仮想計算機をつくるパケットフィルタモジュールを少くとも一つのネットワークエンティティに設ける段階、上記ネットワーク内の上記パケットの流れを許可または拒否するために上記パケットフィルタリングモジュール仮想計算機を動作させるために上記モジュールが上記命令を読取って実行する段階、を含む方法により与えられる。

【００１３】本発明の他の観点はデータがデータパケッ

5

トとして伝送されるコンピュータネットワーク用の保安システムであって、保安ルールに従って上記ネットワーク内の上記データパケットの伝送を制御し、この保安ルールにより制御される上記ネットワークの夫々のアスペクトをこの保安ルールがそれらアスペクトで定義し、そしてフィルタ言語命令に変換するようになった保安システムにおいて、上記保安ルールにより制御されるべき上記ネットワークの少くとも一つのエンティティに、上記データパケットの伝送を制御するパケットフィルタリング仮想計算機をつくるパケットフィルタモジュールを設ける段階、上記ネットワーク内の上記パケットの伝送を許可しまたは拒否するために上記パケットフィルタリングモジュールを動作させるために、上記モジュールが上記命令を読取り実行する段階を含む。

【００１４】本発明の更に他の観点はデータがデータパケットとして伝送されるコンピュータネットワーク内の保安システムであって、保安ルールに従って上記ネットワーク内の上記データパケットの伝送を制御し、この保安ルールにより制御される上記ネットワークの夫々のアスペクトをこの保安ルールがそれらアスペクトで定義しそしてフィルタ言語命令に変換するようになった保安システムにおいて、上記保安ルールにより制御されるべき上記ネットワークの少くとも一つのエンティティに、上記データパケットの伝送を制御するパケットフィルタリングモジュールをエミュレートするパケットフィルタモジュールを設ける段階、パケットフィルタリング動作用に上記モジュールが命令を読取り実行する段階、その結果を記憶装置に記憶する段階および記憶された結果を利用して上記ネットワーク内のパケットの流れを許可または拒否するように上記パケットフィルタモジュールを動作させる段階を含むシステム運用方法を含む。

【００１５】

【実施例】図１は一例としてのネットワークトポロジを示す。この例では主サイト１００はワークステーション１０２の形のシステム管理機能を含む。このワークステーション１０２はワークステーション１０４、経路指定ルータ１１０およびゲートウェー１０６を含むネットワークに接続する。経路指定ルータ１１０は衛星１１２およびゲートウェー１２２を介して遠隔サイトに結合する。ゲートウェー１０６は経路指定ルータ１０８を介してインターネットに接続する。遠隔サイト１２０はワークステーション１２４を含み、これらワークステーションはネットワークにそしてゲートウェー１２２を介してインターネットに接続する。図示の構成は例であり、本発明を適用しうるネットワークのタイプを限定するものではない。そのようなネットワークの構成の数は無限であり、それら構成をつくる技術は当業者には周知である。本発明はそれらの構成のいずれについても動作しうる。

【００１６】図２は本発明を適用した図１のネットワーク

6

を示している。図２において、図１と同じ要素には同じ参照数字を付して示してある。図示のように、システム管理部１０２は制御モジュール２１０、パケットフィルタ発生器２０８、表示装置２０６、記憶媒体２１２を含む。パケットフィルタ２０４はシステム管理プログラム、ワークステーション１０４およびゲートウェー１０６に設けられる。ゲートウェー１０６は２個のそのようなフィルタを有し、その一方はそのネットワークへの接続点に、他方は経路指定ルータ１０８への接続点にある。ルータ１０８と１１０は夫々この保安システムにより発生されるが本発明の部分ではないプログラミングスクリプトテーブルを有している。これらテーブルは当業者には周知のようにルータをプログラムするために現在利用されるテーブルに対応する。

【００１７】パケットフィルタ２０４は遠隔サイト１２０のゲートウェー１２２にも設けられる。１個のパケットフィルタは衛星１１２とゲートウェー１２２の間に、他のパケットフィルタはインターネットとゲートウェー１２２の間にそして第三のパケットフィルタはゲートウェートとネットワークの間に設けられる。

【００１８】情報は当業者には周知のようにパケットの形でネットワークを流れる。図２のパケットフィルタの位置は、ワークステーション、ルータまたはゲートウェーのようなネットワークの特定のオブジェクトに対するデータの流れが制御されうるように選ばれる。このように、夫々のワークステーション１０４はそれに対する情報流が別々に制御されるように一つのパケットフィルタを有する。しかしながら、遠隔サイト１２０においては、パケットフィルタはゲートウェー１２２とネットワークの間の接続部に配置されるから、ワークステーション１２４に対するデータの流れを個々には制御しない。そのような個々の制御が必要な場合には各ワークステーション１２４にも配置されることになる。夫々のパケットフィルタは、ネットワークがつくられあるいは保安システムが設置される時点で設置される。しかしながら付加的なパケットフィルタは後に設置しうる。これらパケットフィルタは保護を要するワークステーションまたはゲートウェーのようなホスト装置に設置される。

【００１９】各パケットフィルタはシステム管理部１０２内のパケットフィルタ発生器２０８により発生された一群の命令にもとづき動作する。これら命令は、パケットの許可または拒否用のパラメータを含むテーブルに対してパケットの内容を単にチェックするのではなく、そのパケットについて複合的動作を行いうるようにする。このように各パケットフィルタは大きなフレキシビリティをもって保安ルールの変更を扱うと共にパケットフィルタ自体の構造を変えることなく複数の保安ルールを扱うことが出来る。

【００２０】システム管理部は、モニタ２０６に表示されそして図３について詳述するように、図形ユーザーイ

ンターフェース（ＧＵＩ）を介して保安ルールに入る。この情報はパケットフィルタ発生器２０８により処理されそして、その結果のコードが希望の機能を行うようにネットワーク内の適正なパケットフィルタに送られる。制御モジュール２１０はシステム管理部がネットワークの動作に追従しうるようにし、記憶装置２１２はそのネットワークの動作そしてそのネットワークへの不法なエントリの試みをログに維持するために利用される。システムオペレータはそれによりネットワークの動作および保安ルールの成功と失敗についての安全なリポートを与えられる。これにより、保安管理部はそのネットワークの接続性を制限することなくそのネットワークの安全性を維持するために適正である変更を行うことが出来る。

【００２１】図３は図２のコンピュータスクリーン２０６を詳細に示す。このスクリーンは４個のウィンドー、すなわち左側の２個の小さいウィンドーと右側の２個の大きなウィンドー、に分けられる。ネットワークオブジェクトおよびサービスは本発明の保安方法で定義されねばならないネットワークの二つのアスペクトである。ウィンドー３０４はシステムに接続するワークステーション、ゲートウェーおよび他のコンピュータハードウェアのようなネットワークオブジェクトを限定するために用いられる。また例えば、会社の財務部、研究開発部および取締役のような種々のデバイスを群化することも出来る。このようにネットワーク上の個々のコンピュータのみならず、ネットワーク上のコンピュータ群へのデータを適正なパケットフィルタの配置により制御することが出来る。これはシステムオペレータにネットワーク上の通信の管理において大きなフレキシビリティが与えられるようにする。例えばＣＥＯや取締役のような会社の財務主任並びに他の高位の社員が財務部と直接的に通信しうるようにし、他のグループからの通信を排除することが出来る。また、すべてのグループからの電子メールは許すが特定のコンピュータ群に対する他の情報要求を制限することも出来る。これによりシステムオペレータはそのネットワークについて内外の安全性を与えうるようになる。このオブジェクト定義はネットワーク上のオブジェクトのアドレス並びにそのオブジェクトがそのネットワークについて内部であるか外部であるかについての名前またはグループ、パケットフィルタがそのオブジェクトに設置されているかどうかについての名前またはグループ、および図形記号を含む。図形記号はルールベース管理部３０２に関連して用いられる。

【００２２】同様に、ネットワークサービスはスクリーン上のブロック３０６で定義される。これらネットワークサービスは例えばログイン（login）、ルート、システムログ、テルネット（telnet）を含むことが出来る。各サービスは一般および特殊特性により限定される。一般特性は例えばテルネットについては２３であるサービス“ｄｐｏｒｔ（宛先ポート）”を識別するコードストリングを含む。入力パケット、出力パケットを識別するコードストリングが識別される。特殊特性はサービス名、サービスを与えるために用いられるポート、無接続セッションが非活動のままである時間についてのタイムアウト（秒）、すなわち、そのセッションが完了したとされる前にいずれかの方向にパケット伝送がない時間、を含む。サービス定義の他のエレメントはＲＰＣサービスについてのプログラム番号およびＵＤＰのような無接続プロトコルを用いる許可されたサービスについてのアウトバウンド接続を含む。

【００２３】ブロック３０２は新しい保安ルールが図形的システムに入りうるようにしそれによりシステム管理部が特定の保安ルールを行うまたは保安ルールを変更するためのコードの書込みをしないですむようにする、ルールベース管理部である。システムに新しいルールを入れるには４個のエレメントがあればよい。第１エレメントはデータパケットのソースであり、第３エレメントはそのパケットの宛先である。第２エレメントは関連するサービスのタイプであり、第４エレメントは行われるべきアクションである。このアクションはパケットの許可でありその場合パケットはソースから宛先に通され、あるいはパケットの拒否でありその場合にはパケットはソースから宛先に通らない。パケットが拒否された場合、アクションは生ぜずあるいはそのパケットが宛先に通されなかったことを示す否定応答を送ることが出来る。更に、特定されうるもう一つのエレメントはどのオブジェクトについてルールが適用されるのかを特定するルールについての設置位置である（図２参照）。設置位置が特定されなければシステムは省略により通信宛先にパケットフィルタモジュールを置く。これらオブジェクトは必ずしも宛先である必要はない。例えば、インターネットから局所ホストに宛てた通信は必ずゲートウェーを通る。それ故、そのゲートウェーがソースでもなく宛先でもない場合であっても、ゲートウェーにルールを適用することが出来る。頭字語（acronyms）または図形記号を伴うデータを入れることにより、各ルールは高速で入れられそしてこの目的のために新しいコードを書込み、コンパイルしそしてチェックする必要なしに検査されうる。このように、システム管理部は保安目的についてのコンピュータのプログラミングに際してエキスパートである必要はない。サービスがシステムにすでに入っているサービスの内の一つである限り、システム管理部の機能についてホストとしてサービスするコンピュータはその情報を、後述するように適当なパケットフィルタ用の一群の命令へと処理する。

【００２４】ブロック３０８は保安システムの構成と動作を要約するシステムスナップショットである。本発明を実施する必要はない。このシステムスナップショットは図形記号を用いてシステムの要約を表示する。例えば、この要約はホストアイコン、ホスト名、ルールベー

スを含むファイル名であるルールベース名およびルールベースがホストに設置された日付を含むことが出来る。またこれはホストとの通信があったかどうかを示すホストの状態並びにホストにより検査され、ドロップされそしてログされたパケットの数をも示すことが出来る。

【００２５】図４はＧＵＩ上の情報を、パケットフィルタ用に利用されるルールを含むフィルタスクリプトに変換するサブシステムのフローチャートである。この実施例においては、フィルタスクリプト発生器の出力は後述のようにそのときパケットフィルタモジュールにより行われるオブジェクトコードにコンパイルされる。

【００２６】サブシステム４００は４０２でスタートし、ブロック４０４に移り、ここでＧＵＩから第１ルールを獲る。第１ルールはスクリーンの第１ラインであって、そこで図３に示すように新しい保安ルールが識別される。次に制御はブロック４０６に移り、そこでそのルールソースをネットワークオブジェクトに一致させるためのコードが発生される。すなわち、データパケットが出るシステムのオブジェクトの一つを表わすものとしてパケットのソースがソースコードブロックに入れられる。次に制御はブロック４０８に移り、ネットワークのどのオブジェクトにデータパケットが宛てられるかを示すためのコードが宛先コードブロック内に発生される。次に制御はブロック４１０に移り、選ばれたルールサービスを一致させるためのコードが発生される。これらルールサービスは予め定義されておりそしてシステム内に記憶されるか、あるいは定義されていなければ、そのサービスを調整する保安ルールがシステムに入れられるときに定義される。次に制御はブロック４１２に入り、データブロック４０６，４０８および４１０が一致したとき、すなわちチェックの結果が真であるときパケットを許可するためまたは拒否するためのコードが発生される。許可または拒否のためのアクションは保安ルールにおいて選ばれたアクションにもとづく。次に制御は決定ブロック４１４に入り、システムに他のルールを入れるべきかどうかを決定する。他のルールをシステムに入れるべきでない場合には制御はブロック４１６に入り、次のルールを得てブロック４０６にもどり、そのときプロセスがくり返されそしてＧＵＩの次のラインである次の保安ルールが処理される。

【００２７】通信プロトコルは階層をなしており、従ってプロトコルスタックとも呼ばれる。ＩＳＯ（International Stndard Organization）は通信プロトコル層の設計用のフレームワークを与える一般モデルを定義している。このモデルは現存する通信プロトコルの機能性を理解するための基本的なリファレンスとして作用している。

ＩＳＯ　ＭＯＤＥＬ

層	機　能	例
7	アプリケーション	Ｔｅｌｎｅｔ，ＮＦＳ，Ｎｏｖｅｌｌ　ＮＣＰ
6	プレゼンテーション	ＸＤＲ
5	セッション	ＲＰＣ
4	トランスポート	ＴＣＰ、Ｎｏｖｅｌ　ＳＰＸ
3	ネットワーク	ＩＰ，Ｎｏｖｅｌｌ　ＩＰＸ
2	データリンク（ハードウェアインターフェース）	ネットワークインターフェースカード
1	フィジカル（ハードウェア接続）	Ｅｔｈｅｒｎｅｔ，Ｔｏｋｅｎ Ｒｉｎｇ，ＴＩ

【００２８】異なる通信プロトコルはＩＳＯモデルの異なるレベルを使用する。或る層内のプロトコルは他の層で使用されるプロトコルには無関係となりうる。これは、保安アクションを行うときの重要な因子である。例えば、アプリケーション（レベル７）は通信の試み（レベル２－３）についてソースコンピュータを識別出来ず、それ故充分な保安性を与えることが出来ない。

【００２９】図５はＩＳＯモデルにおいていかにして本発明のフィルタパケットモジュールを用いるかを示している。ＩＳＯモデルの通信層は図５の左側に５０２で示してある。レベル１、ブロック５０４、はネットワークの種々のオブジェクトを接続するために用いられるワイヤでよいネットワークのハードウェア接続である。第２レベル、図５のブロック５０６、はネットワークの各コンピュータに配置されるネットワークインターフェースハードウェアである。本発明のパケットフィルタモジュールはこのレベルと、ネットワークソフトウェアであるレベル３との間に入る。また、ＩＳＯモデルの他のレベルは一つのセグメントから次のセグメントにデータを配布することに関連するレベル４、ブロック５１０、およびネットワーク上の“セッション”の開閉を同期させるレベル５、ブロック５１２である。レベル６、ブロック５１４はネットワーク上の種々のコンピュータ間のデータの変化に関係し、レベル７、ブロック５１６はアプリケーションプログラムである。

【００３０】パケットフィルタモジュールのあるコンピュータに入るパケットはレベル１と２を通り、図５の右側に示すパケットフィルタ５２０に入る。このパケット

はブロック５２２に入る。ブロック５２４においてこのパケットは保安ルールと比較され、そしてそのパケットがルールと一致するかどうかについての決定がなされる。このパケットとルールが一致すれば、システム管理部のログに入れられそして、システムに入れるための不法な試みがなされたとすれば、アラートが出される。次に制御はブロック５３４に入り、保安ルールの要件にもとづきこのパケットを通すかどうかの決定がなされる。パケットを通す決定がなされれば、そのパケットはレベル３、ブロック５０８に通る。このパケットを通さない決定がなされると、もしこのオプションが選ばれれば否定応答（ＮＡＣＫ）がブロック５２８に送られ、そして制御はブロック５３０に移り、そのパケットがドロップされる、すなわちその宛先に通されない。同様に、アプリケーションが他の宛先に送られるべきパケットを発生するとすれば、そのパケットはレベル３、ブロック５０８でＩＳＯモデルを出てブロック５２２に入り、そのパケットが通されるべきときにレベル３、ブロック５０８ではなくレベル２、ブロック５０６に通される点を除き同じプロセスにより処理される。レベル２において、パケットはブロック５０４でレベル１に送られる。このパケットがルールと一致しなければ、次のルールがとり出されてそれと一致するかどうかについて検査される。ソース宛先または特定されるサービスには無関係に任意のパケットを一致させる省略ルールが与えられる。他のルールが一致しないとき、このルールがとり出されてそのパケットをドロップさせる。パケットのドロップはこのような場合にとられる最も安全なステップである。勿論“エンプティルール”をパケットの通過のために書込んでもよい。

【００３１】図６において、６００は図５のブロック５２０の詳細を示す。図６における一般的な説明と図７～図１０に示すより詳細な説明は用語“パケットフィルタモジュール”を定義するものである。これらの図に示す能力はパケットフィルタモジュールの最少の動作能力である。図１１～図１５はこのパケットフィルタモジュールに含まれうるが用語の最少定義には必要ない付加的な特徴を示す。

【００３２】パケットフィルタモジュールはここではネットワーク上の一つのコンピュータであるホストコンピュータにある、図６～図１０に示すマシンのエミュレーション（emulation)として定義される“仮想計算機”として具体化される。

【００３３】仮想計算機は図５のブロック５２２に対応するブロック６０２でスタートし、パケットを受信する。制御はブロック６０４に移り、フィルタ動作がメモリ（図示せず）からの命令から得られる。これらフィルタ動作は図２のパケットフィルタ発生器２０８により発生されたフィルタ動作である。次に制御はブロック６０４に入りそこでフィルタ動作が得られそしてブロック６０６に入りメモリ６１８が初期化される。ブロック６０８において、第１仮想計算機動作が得られそしてブロック６１０で行われる。この仮想計算機は中間値の記憶に用いられるスタックまたはレジスタ６１８のようなメモリ機構を含む。このスタックまたはレジスタの利用は表１に関連して詳述する。次に制御は決定ブロック６１４に入り、ストップ状態となったかどうかが決定される。ストップ状態になっていれば次の決定はそのパケットを許可するか拒否するかであり、その決定はブロック６１６で行われる。パケットが通されていればそのパケットは図５に示すように進む。パケットが拒否されれば、それはドロップされ、そしてブロック５２８と５３０に示すように否定応答が送られる。ブロック６１４でストップ状態になっていなければ、次の動作はブロック６１６で得られそしてプロセスはブロック６１０からくり返される。

【００３４】ステップ５、ブロック６１０、で行われる動作のタイプは図７に示してある。図７において、ブロック６１０と６１４は図６に示すものと同じである。接続６１３は並列に示す３つの動作により割込まれる。ブロック６１０で行われるべき動作について、制御は適正なブロック７０２，７０４または７０６に入り、タスクを行う。ブロック７０２において、データ抽出が行われ、ブロック７０４では論理演算が行われ、ブロック７０６では比較動作が行われる。図７の右側に示すように、他のブロックは仮想計算機により行うことの出来る動作に並列に加えることが出来る。ブロック７０２，７０４，７０６に示すサブセットは本発明の仮想計算機の重要なエレメントである。これらエレメントは夫々図８、９、１０に詳細に示してある。仮想計算機により行うことの出来る動作にオプションとして含めることの出来る付加エレメントは夫々図１１～図１５に示してある。

【００３５】データ抽出ブロック７０２は図８に詳細に示す。このプロセスはブロック８０２でスタートし、次にブロック８０４でパケット８０６内の特定のアドレスからデータが抽出される。このアドレスはスタックメモリ６１８または命令コードからとり出される。抽出されるデータの量もこのスタックメモリまたは命令コードにより決定される。抽出されたデータはブロック８０８でメモリスタック８１０に置かれる。このプロセスはブロック８１２で終了する。これら図面において、制御の流れは単線矢印で、データの流れは二重線矢印で示す。

【００３６】図９は論理演算７０４を詳細に示す。この演算はブロック９０２でスタートし、ブロック９０４でメモリ９０６から第１値が得られる。ブロック９０８でそのメモリから第２の値が得られ、そして論理演算がブロック９１０で行われる。この論理演算が真であればブロック９１２でメモリ９０６に１が置かれ、誤であればブロック９１４でメモリ９０６に０が置かれる。このプ

ロセスはブロック９１６で終了する。

【００３７】仮想計算機に要求される第３であって最後の動作を図１０に示す。この比較動作、ブロック７０６、はブロック１００２でスタートし、ブロック１００４で第１値がメモリ１００６より得られる。次にブロック１００８で第２値がメモリ１００６より得られる。第１および第２値間の比較がブロック１０１０で行われる。その結果が真であればブロック１０１２でメモリ１００６に１が置かれ、誤であればブロック１０１４で０が置かれる。このプロセスはブロック１０１６で終了する。

【００３８】次の動作は図７には示していないが、同図の右側に破線で示すように付加されるものであって、ブロック７０２，７０４，７０６と同様に、すなわち並列に接続される。図１１はリテラル値のメモリへのロードを示す。このプロセスはブロック１１０２でスタートし、次にブロック１１０６で命令コードからリテラル値が得られる。この値はブロック１１０８でメモリに置かれそしてこのプロセスはブロック１１１０で終了する。

【００３９】条件付ブランチ動作を図１２に示す。このプロセスはブロック１２０２でスタートし、次にブロック１２０４で命令コードからとり出されたブランチ条件がチェックされる。このブランチ条件がブロック１２１０において真であれば、ブロック１２０８でその値がメモリスタック１２０６から得られる。ブロック１２１０の比較結果が真であれば次のステップはＮにセットすることであり、このプロセスはブロック１２１６で終了する。ブロック１２１０での比較が誤であればブロック１２０４において制御はブロック１２１４に入る。

【００４０】算術またはビット形の演算を図１３に示す。このプロセスはブロック１３０２でスタートし、次にブロック１３０４でメモリ１３０６から第１値が得られる。ブロック１３０８でメモリ１３０６から第２値が得られ、そしてブロック１３１０でメモリから得られたこれら二つの値についての算術またはビット型の演算が行われる。この演算の結果はブロック１３１２でこのメモリに置かれ、そしてこのプロセスはブロック１３１４で終了する。

【００４１】図１４は、データが保安ルールを実行する第１群の命令から第２保安ルールについての第２群の命令に通すべきときに有用なルックアップ動作である。図６のブロック６０６に示すように、新しい保安ルールが処理されるときにメモリが初期化される。それ故、第１の保安ルールによりメモリに置かれた情報は第２保安ルールによる使用には供されない。この問題を克服するために、別のメモリ１４１０が与えられる。これはこの目的に利用されるテーブル１～３を含む。これらテーブルへのデータエントリは図１５に示されており、以下これを説明する。ルックアップ動作は１４０２でスタートし、次に１４０４においてメモリ１４０６から値が得られる。次にブロック１４０８においてブロック１４１０のテーブル１～３から参照されるテーブル内の値をサーチすることによりデータが得られる。次にブロック１４１２でそのブロックがそのテーブルにあるかどうかの決定がなされる。この決定がＹであればブロック１４１６でメモリ１４０６に１が置かれ、Ｎであればブロック１４１４で０が置かれる。このプロセスはブロック１４１８で終了する。

【００４２】図１５において、このプロセスはブロック１５０２でスタートし、次にブロック１５０４でメモリ１５０６から値が得られる。次にブロック１５０８でメモリ１５０６からの値がブロック１５１０のテーブル１～３内の適当な位置に置かれる。次にブロック１５１２でテーブルに記憶された値が成功したかどうかの決定がなされる。成功であればブロック１５１６でメモリ１５０６に１が置かれ、そうでなければブロック１５１４で０が置かれる。このプロセスはブロック１５１８で終了する。

【００４３】保安ルールの一例は本発明のパケットフィルタリング方法を用いて行われる。それをシステム内のどのテルネット（Telnet）サービスをも許可しないようにする保安ルールを一例として次に述べる。テルネットはＴＣＰサービスとして定義されそして特定のＴＣＰ宛先ポートを有する。これはパケットのバイト位置９にＴＣＰプロトコル値６を有することおよびパケットのバイト位置２２に宛先テルネットプロトコル数２３を有することで識別される。この値は２バイト値である。これはすべてのテルネット要求パケットにある。

【００４４】テーブル１内の第１の動作はパケット位置９からＩＰプロトコルを抽出し、そしてそれをメモリに置くことである。テーブル１の右側の“メモリ値”の欄に示すように、この値６はスタックの上に置かれる。第２の動作、すなわち、上記した６であるＴＣＰプロトコル（ポート）番号はメモリの第２の位置に置かれる。ステップ３において、このスタックのはじめの２層の値が比較されて正の結果を得る。

【００４５】

【表１】

15　　16

テーブル１
ドロップテルネットプロセス

#	パケットフィルタコード	仮想計算機動作	メモリ値（スタック順）		
1	ｐｕｓｈ ｂｙｔｅ［9］	抽出動作：パケット位置９からＩＰプロトコル番号をメモリに抽出	6		
2	ｐｕｓｈ６	メモリにリテラル値そう入：ＴＣＰプロトコル数をメモリに置く	6	6	
3	ｅｑ	比較動作：ＴＣＰに対しＩＰプロトコルを比較し、正値を得る	1		
4	ｐｕｓｈｓ［２２］	抽出動作：パケット位置２２からＴＣＰプロトコル数をメモリに抽出	1	２３	
5	ｐｕｓｈ２３	メモリにリテラル値をそう入：ＴＥＬＮＥＴプロトコル数をメモリに置く	1	２３	２３
6	ｅｑ	比較動作：ＴＥＬＮＥＴに対しＴＣＰプロトコルを比較し、正の結果を得る	1	1	
7	ａｎｄ	論理演算：ＴＣＰとＴＥＬＮＥＴが一致したかどうかプロトコルをチェック	1		
8	ｂｔｒｎｅ ｄｒｏｐ	条件付ブランチ動作：メモリ値が真ならドロップ状態にブランチする			

スタックの上の２層における値６は削除され、そして正の結果を示す１がスタックのトップに置かれる。ステップ４でパケット位置２３についてのＴＣＰプロトコル数が抽出されてスタックの第２層のメモリ位置に置かれる。ステップ５でテルネットプロトコル数であるリテラル値がスタックの第３層のメモリに置かれる。ステップ６でテルネット用のＴＣＰプロトコルを含むメモリ層２と３が期待値と比較されて正の結果を得る。このスタックの第２、３層の値が削除され、正の結果を示す１が置かれる。ステップ７でＴＣＰとテルネットの両方が一致したかどうかを見るために論理演算が行われる。これはＡＮＤ動作により決定される。この場合、結果は正であり、スタックのはじめの２層の１は削除され、正の結果を示す１が置かれる。ステップ８で条件付ブランチ動作が行われ、メモリ値が真であればこのプログラムがドロップ状態にブランチする。この場合、結果は正であり、プログラムはドロップ状態にブランチし、テルネット要求は通されない。このようにテルネットを落すためのこのルールは行われる。

【００４６】本発明の特定の実施例について述べたが、或る種の変更が本発明の範囲内で可能なことは当業者には明らかである。例えば上記ではパケットフィルタ動作はスクリプトとして発生されそして次にオブジェクトコードへとコンパイルされたが、それら命令は直接にオブジェクトコードとして発生されてもよく、あるいはスクリプトをオブジェクトコードにコンパイルする必要を避けるためにインタープリータを使用してもよいことは当業者には明らかである。また、仮想計算機の動作を等価的に行うことも当業者には明らかである。例えば、比較動作は変数から一つの値を減算し、その結果について等化操作を行うことにより行うことが出来る。

【図面の簡単な説明】

【図１】ネットワークトポロジーの一例である。

【図２】図１のネットワークトポロジーに適用した本発明の保安システムを示す図。

【図３】図２のネットワーク管理部のコンピュータスクリーンを詳細に示す図。

【図４】図形情報をフィルタスクリプトに変換するためのサブシステムのフローチャート。

【図５】本発明を用いるコンピュータネットワークにおける情報の流れを示す図。

【図６】図５のパケットフィルタの動作のフローチャート。

【図７】図６のパケットフィルタの動作のフローチャート。

【図８】図７の仮想計算機動作を示すフローチャート。

【図９】図７の論理演算法のフローチャート。

【図１０】図７の比較動作法のフローチャート。

【図１１】リテラル値をメモリに入れる方法のフローチャート。

【図１２】条件付ブランチ動作のフローチャート。

【図１３】算術およびビット型演算のフローチャート。

17 18

【図１４】ルックアップ動作のフローチャート。

【図１５】レコード動作のフローチャート。

【符号の説明】

１００　主サイト

１０２，１０４　ワークステーション

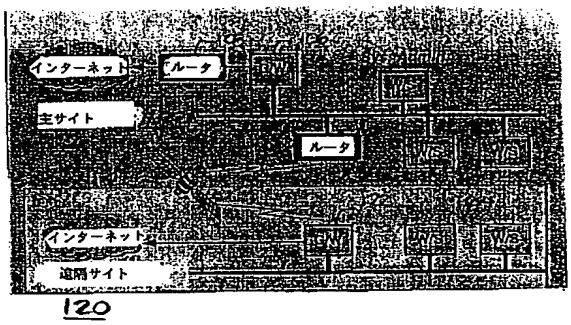
１１０　ルータ

１０６　ゲートウェー

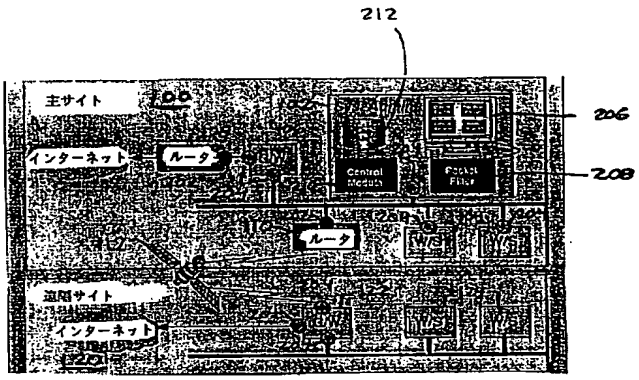
１１２　衛星

１２０　遠隔サイト

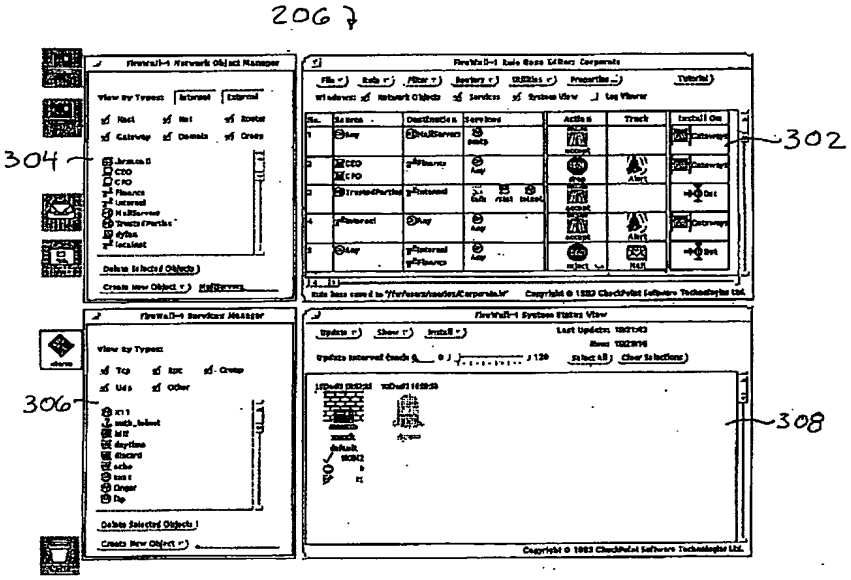
【図１】



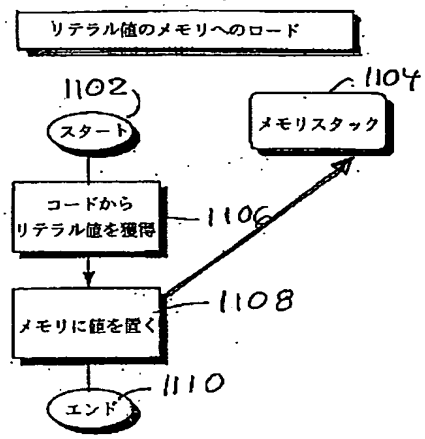
【図２】



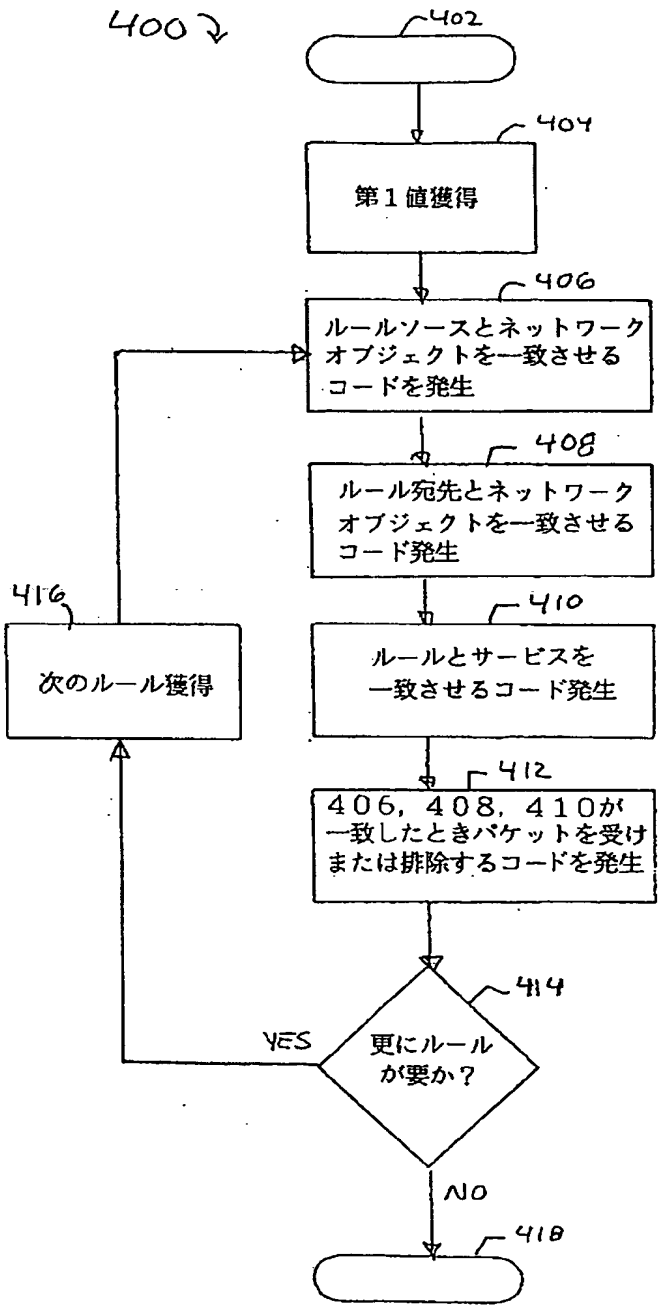
【図３】



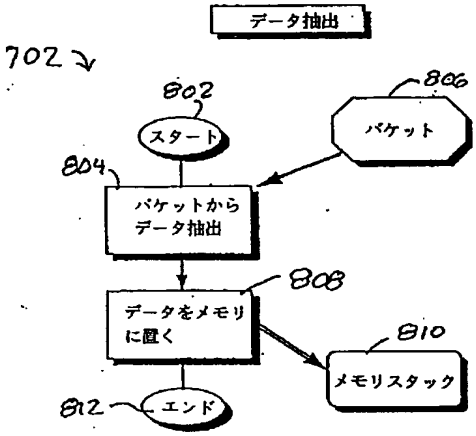
【図１１】



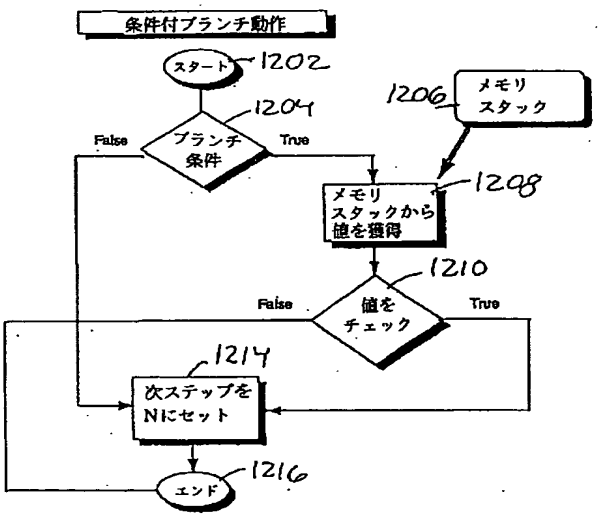
【図４】


400
402
404
第１値獲得
406
ルールソースとネットワークオブジェクトを一致させるコードを発生
408
ルール宛先とネットワークオブジェクトを一致させるコード発生
410
ルールとサービスを一致させるコード発生
412
406，408，410が一致したときパケットを受けまたは排除するコードを発生
414
更にルールが要か？
YES
NO
416
次のルール獲得
418

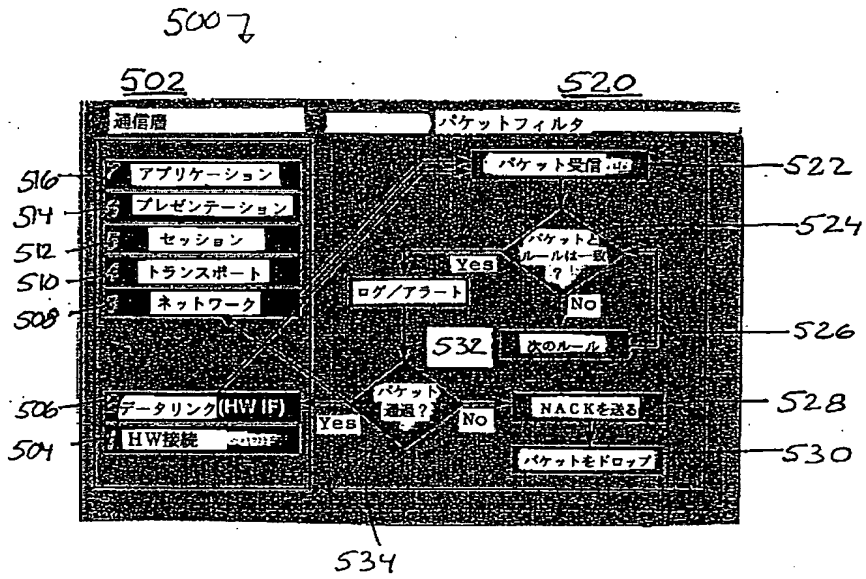
【図８】


データ抽出
702
802
スタート
806
パケット
804
パケットからデータ抽出
808
データをメモリに置く
810
メモリスタック
812
エンド

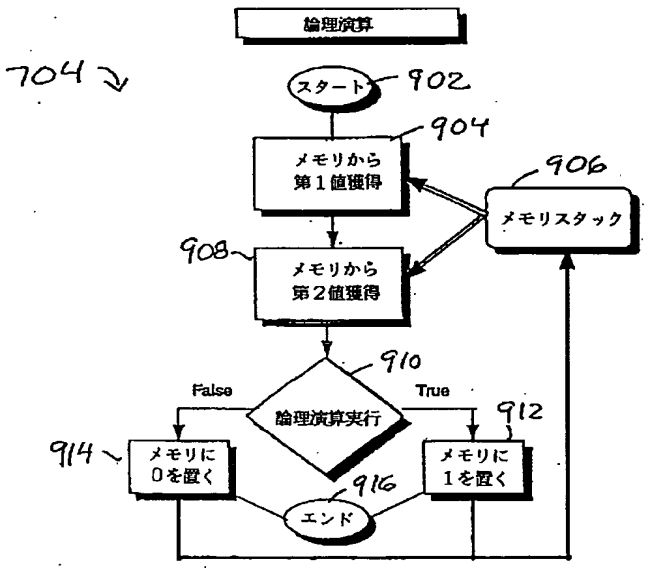
【図１２】


条件付ブランチ動作
スタート
1202
1204
ブランチ条件
False
True
1206
メモリスタック
1208
メモリスタックから値を獲得
1210
値をチェック
False
True
1214
次ステップをNにセット
エンド
1216

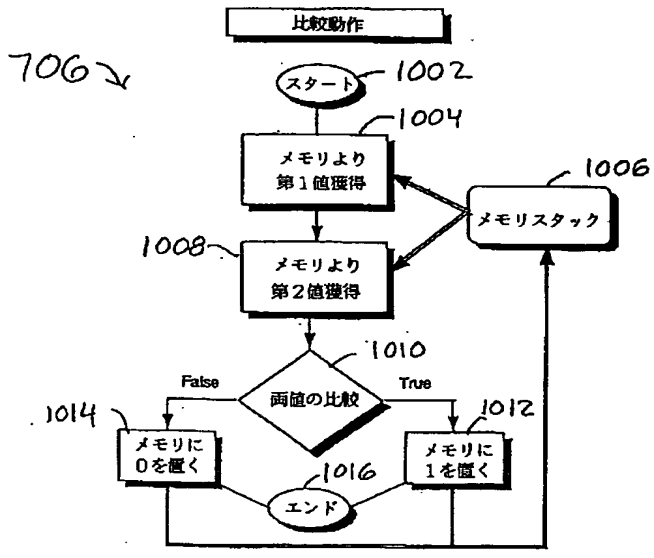
【図５】


500
502
520
通信層
パケットフィルタ
アプリケーション
プレゼンテーション
セッション
トランスポート
ネットワーク
データリンク(HW IF)
HW接続
パケット受信
パケットとルールは一致？
Yes
No
ログ/アラート
次のルール
パケット通過？
Yes
No
NACKを送る
パケットをドロップ
516
514
512
510
508
506
504
522
524
526
528
530
532
534

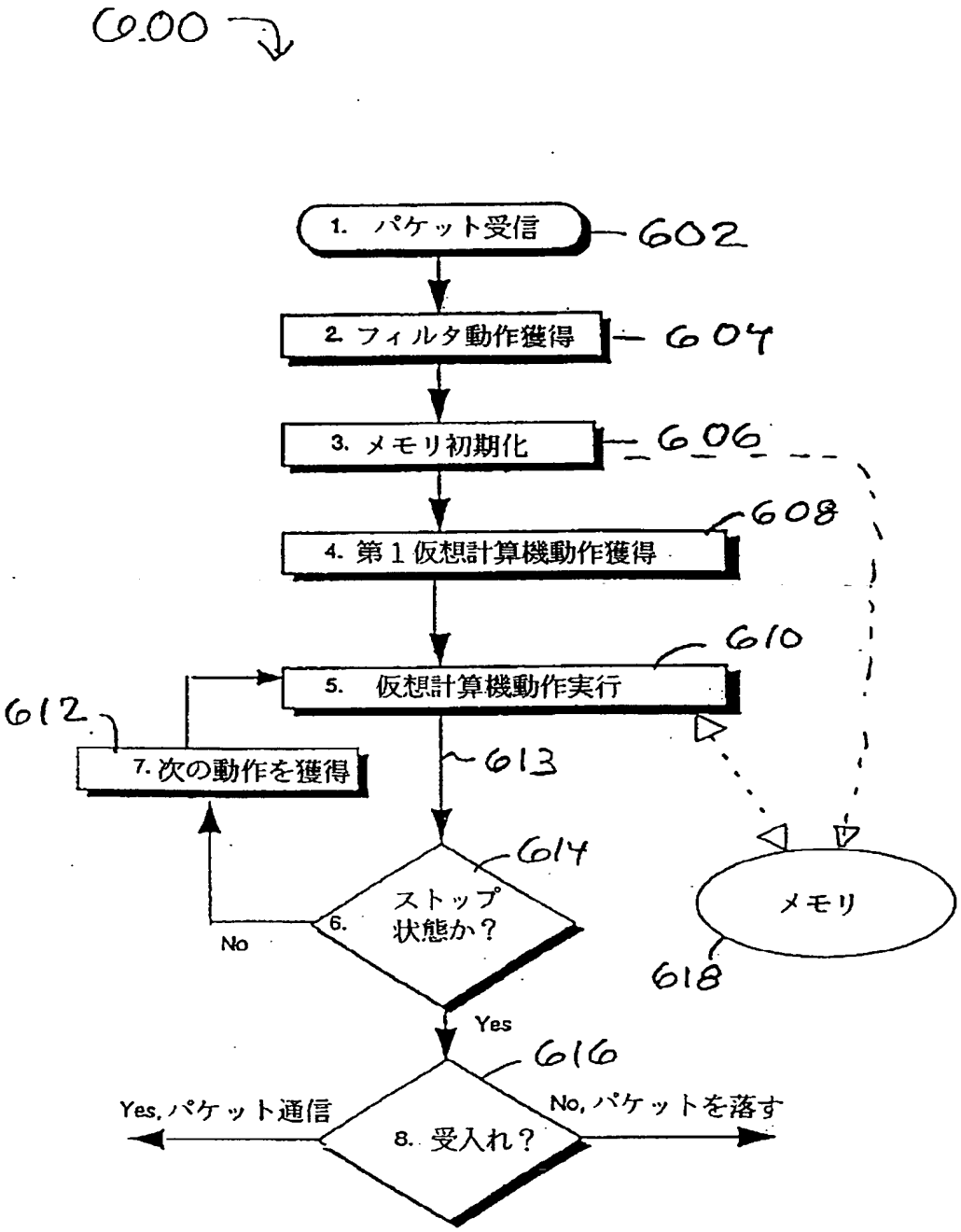
【図９】


論理演算
704
スタート
902
メモリから第１値獲得
904
メモリスタック
906
メモリから第２値獲得
908
論理演算実行
910
False
True
メモリに０を置く
914
メモリに１を置く
912
エンド
916

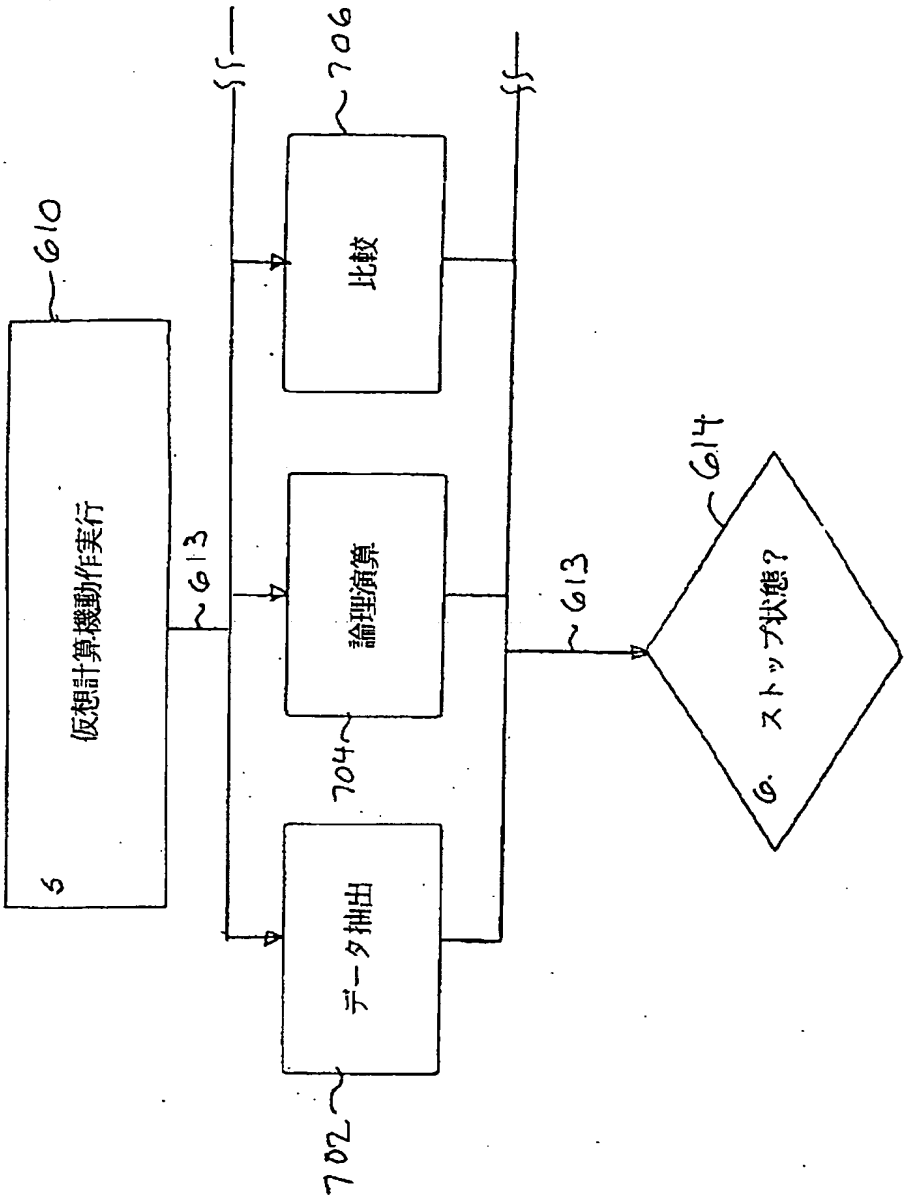
【図１０】


比較動作
706
スタート
1002
メモリより第１値獲得
1004
メモリスタック
1006
メモリより第２値獲得
1008
両値の比較
1010
False
True
メモリに０を置く
1014
メモリに１を置く
1012
エンド
1016

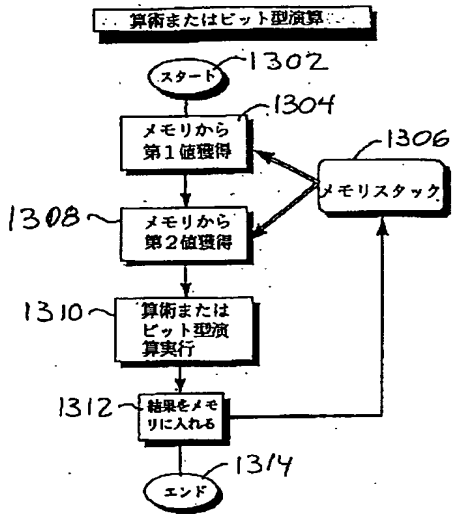
【図６】


600
1. パケット受信
602
2. フィルタ動作獲得
604
3. メモリ初期化
606
608
4. 第１仮想計算機動作獲得
610
5. 仮想計算機動作実行
612
7. 次の動作を獲得
613
614
6. ストップ状態か？
No
Yes
616
8. 受入れ？
Yes, パケット通信
No, パケットを落す
メモリ
618

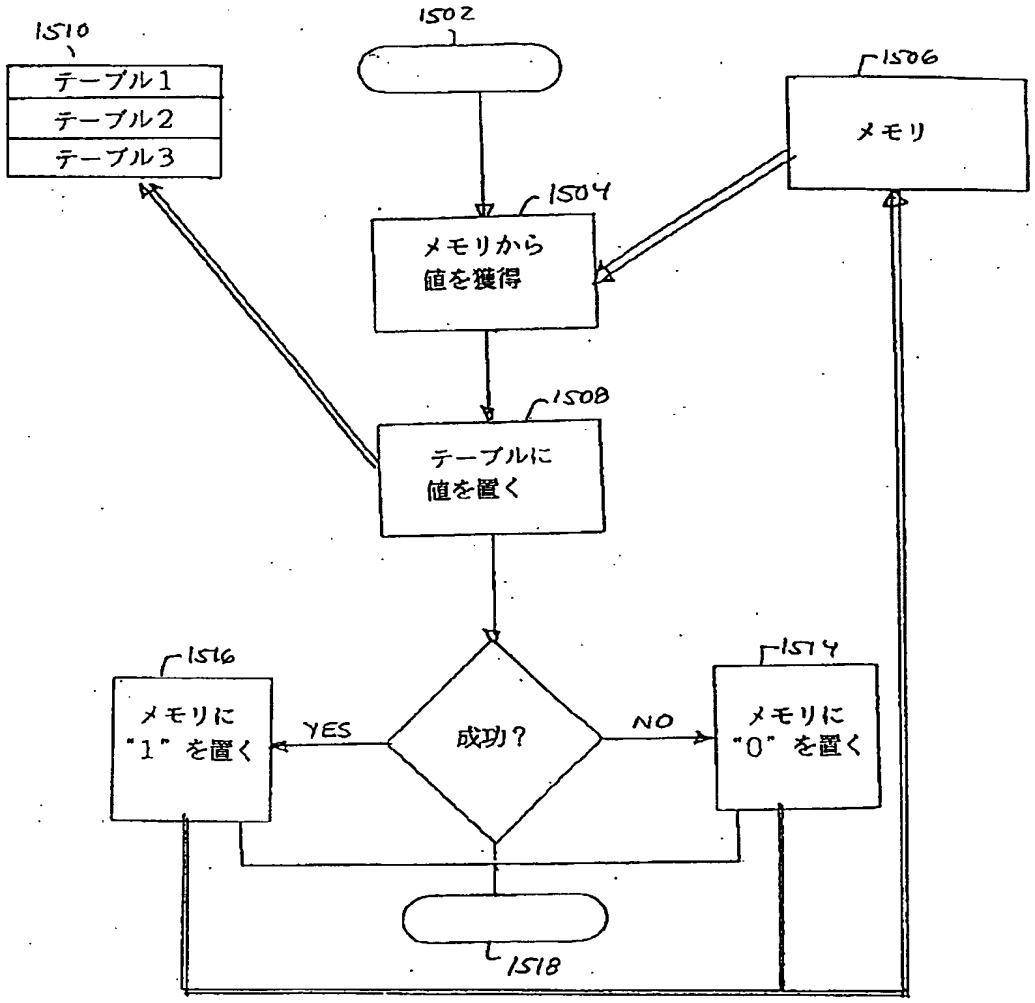
【図７】



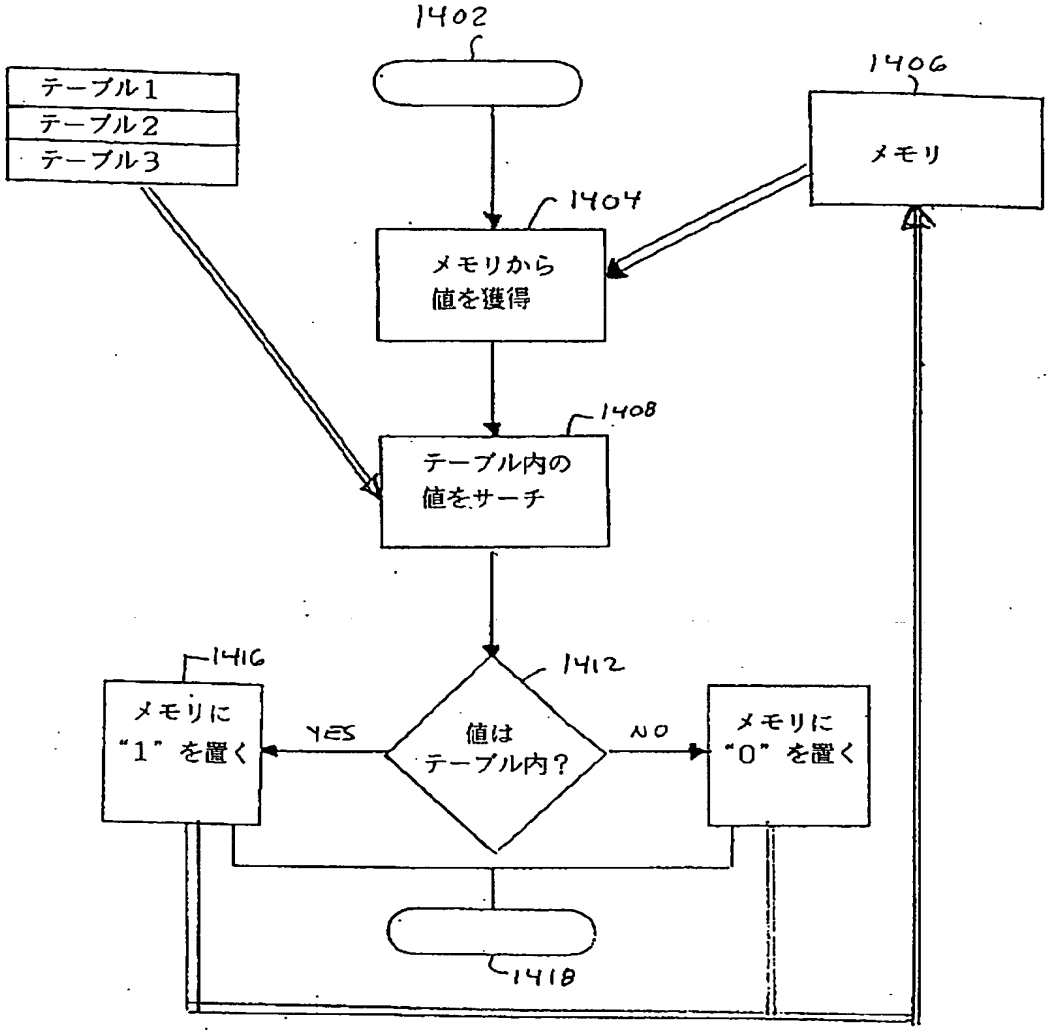
【図１３】


算術またはビット型演算
スタート
1302
メモリから
第１値獲得
1304
メモリスタック
1306
1308
メモリから
第２値獲得
1310
算術または
ビット型演
算実行
1312
結果をメモ
リに入れる
エンド
1314

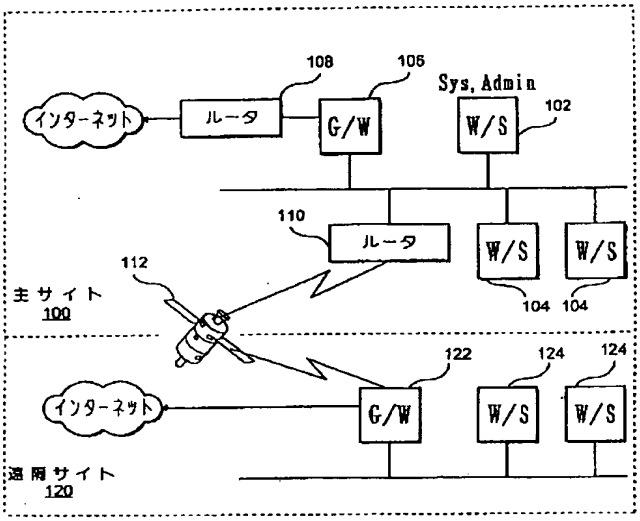
【図１５】


1510
テーブル１
テーブル２
テーブル３
1502
1506
メモリ
1504
メモリから
値を獲得
1508
テーブルに
値を置く
1516
メモリに
"1" を置く
YES
成功？
NO
1514
メモリに
"0" を置く
1518

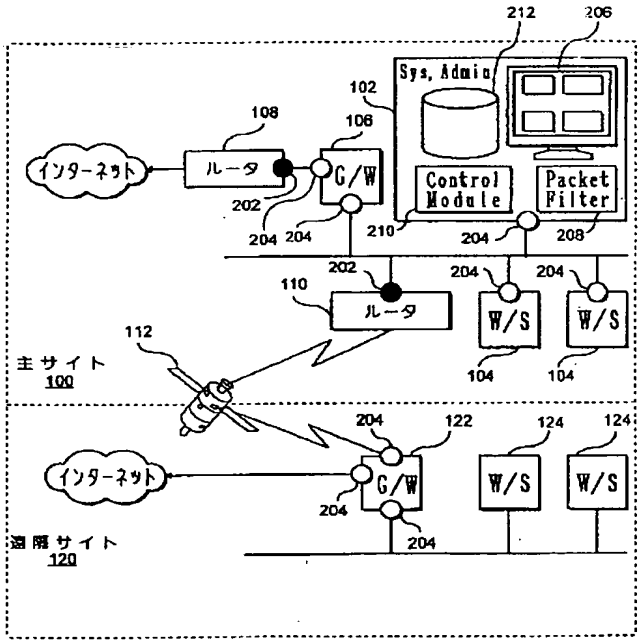
【図１４】



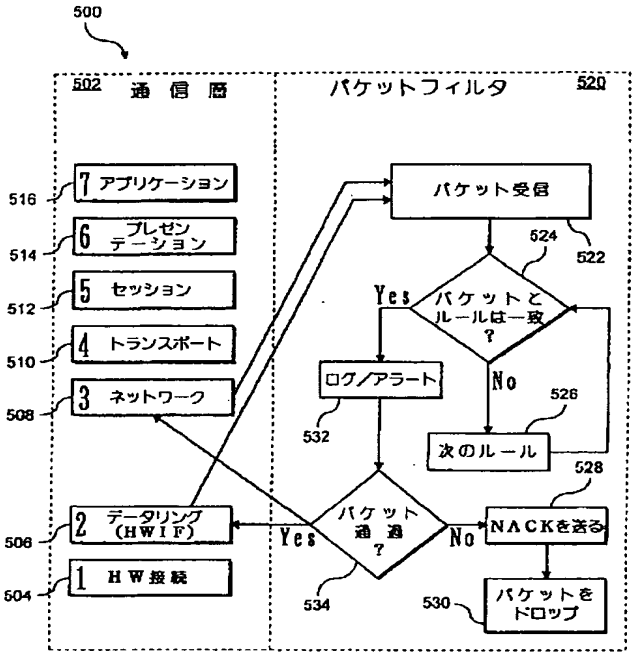
【手続補正書】
【提出日】平成７年５月２日
【手続補正３】
【補正対象書類名】図面
【補正対象項目名】図１
【補正方法】変更
【補正内容】
【図１】



【手続補正４】
【補正対象書類名】図面
【補正対象項目名】図２
【補正方法】変更
【補正内容】
【図２】



【手続補正５】
【補正対象書類名】図面
【補正対象項目名】図５
【補正方法】変更
【補正内容】
【図５】


500
502 通信層
パケットフィルタ 520
7 アプリケーション
6 プレゼンテーション
5 セッション
4 トランスポート
3 ネットワーク
2 データリング (HWIF)
1 HW接続
516
514
512
510
508
506
504
パケット受信
522
524
パケットとルールは一致？
Yes
No
ログ/アラート
532
526
次のルール
528
パケット通過？
Yes
No
NACKを送る
534
530
パケットをドロップ